KEWASPADAAN TERHADAP DOXXING

PENCEGAHAN DAN PERAWATAN UNTUK MEREKA YANG MENJADI TARGET DOXXING DAN INTIMIDASI POLITIK

KEWASPADAAN TERHADAP DOXXING

Pencegahan dan Perawatan untuk Mereka yang Menjadi Target Doxxing dan Intimidasi Politik

Panduan langkah demi langkah ini menjelaskan cara melindungi diri Anda dari penguntit online, mengapa hal itu penting, dan apa yang harus dilakukan jika Anda menjadi sasaran "doxxing"—penyebaran informasi pribadi Anda. Di era pengawasan universal, ketika streaming langsung menyiarkan setiap demonstrasi besar sementara fasis, agen FBI, dan petugas polisi menyisir pos media sosial untuk mengumpulkan intelijen yang dapat digunakan untuk menyerang aktivis, tidak pernah ada waktu yang lebih baik untuk mengambil langkah-langkah untuk mengamankan privasi Anda. Begini caranya.

Apa Itu Doxxing?

Doxxing berarti menyebarkan informasi pribadi seseorang dengan tujuan mengekspos dan mengintimidasi mereka. Hal ini dapat mengakibatkan kerugian fisik, emosional,

dan ekonomi pada target. Hal ini dimaksudkan untuk menghalangi target dari tindakan dan mempermalukan mereka karena ide-ide dan nilai-nilai mereka. Penting untuk memperhatikan keamanan dengan serius sebelum Anda didoxx—bahkan sebelum Anda memiliki alasan untuk takut bahwa Anda bisa didoxx. Seringkali seorang doxxer akan menunggu sampai mereka mengumpulkan banyak informasi sebelum merilisnya. Ada kemungkinan bahwa Anda sudah dikuntit dan tidak akan mengetahuinya sampai terlambat.

Apakah Anda seorang aktivis publik yang terkenal atau hampir tidak terlibat sama sekali, Anda harus melindungi jaringan sosial Anda dan bidang lain dalam hidup Anda—bahkan jika Anda tidak berpikir Anda melakukan sesuatu yang memerlukan perhatian. Mempertahankan praktik yang baik melindungi teman, keluarga, dan komunitas Anda. Adalah umum bagi orang untuk dimasukkan dalam teori konspirasi sayap kanan tentang "anggota Antifa" semata-mata karena mereka queer atau trans, "terlihat seperti kiri," bermain di band, menghadiri acara, atau nongkrong di ruang radikal. Informasi tersebut tidak harus benar atau dibenarkan bagi seseorang untuk menargetkan Anda. Yang dibutuhkan pelaku intimidasi hanyalah satu informasi untuk mulai mencari lebih ba-

nyak detail secara online.

Menyadari jejak informasi apa yang Anda tinggalkan secara online dapat melindungi Anda dari penegak hukum serta penguntit. Sekarang pengawasan yang dipaksakan oleh negara semakin canggih dan streaming langsung telah menjadi normal pada demonstrasi, hanya mengenakan topeng seringkali tidak cukup. Pada Juni 2020 di Philadelphia, penyelidik mengidentifikasi seorang wanita yang dimulai dengan tidak lebih dari foto buram dirinya. Mereka mengikuti jejak remah roti termasuk pembelian Etsy, akun twitter, dan halaman kerja profesionalnya. Bea Cukai dan Petugas Perbatasan sudah mulai menjaring media sosial publik. Mengamankan kehadiran online Anda dapat membuat Anda merasa lebih aman melakukan tindakan offline.

Mencegah Lebih Baik Daripada Mengobati

Tidak ada waktu yang lebih baik untuk memulai daripada sekarang. Setelah Anda didoxx, Anda mungkin tidak dapat menghilangkan informasi yang ada di luar sana bahkan jika Anda mencoba untuk menghapusnya.

Ada banyak cara berbeda untuk mendekati ini. Jelas, cara

terbaik untuk memastikan bahwa tidak ada yang dapat menemukan informasi apa pun tentang Anda adalah dengan tidak memiliki apa pun yang tersedia — tetapi beberapa orang tidak dapat menghilangkan kehadiran online mereka, baik karena pekerjaan, keluarga, atau tanggung jawab lainnya. Dalam beberapa kasus, ada alasan strategis untuk mempertahankan semacam persona online; misalnya, memiliki akun media sosial yang sudah lama, dapat dipercaya, tetapi tidak berbahaya mungkin berguna bagi non-warga negara yang melintasi perbatasan AS. Untungnya, ada cara untuk melindungi berbagai bidang kehidupan Anda, membuat profil publik jika Anda memerlukannya, dan menerapkan praktik yang dapat membantu Anda dan teman Anda merasa diberdayakan untuk terus mengambil tindakan di komunitas Anda. Proses ini bisa membosankan. Itu akan memakan waktu dan tenaga. Saya merekomendasikan melakukannya bersama dengan teman, teman sekamar, atau anggota keluarga untuk membantu melalui beberapa aspek yang sulit atau membosankan.

Mempertahankan Bidang Terpisah

Jika Anda tidak dapat sepenuhnya menghapus diri Anda dari internet, Anda masih dapat menjaga privasi relatif

dengan mempertahankan bidang aktivitas online yang berbeda dan membersihkan akun yang terlupakan atau jarang digunakan.

Anda mungkin memiliki lebih dari satu kehadiran online. Ini dapat mencakup jejaring sosial, papan pesan, situs pekerjaan, akun email—apa pun yang Anda perlukan untuk masuk. Seringkali dalam doxxing, informasi ditriangulasi dari berbagai sumber. Salah satu cara untuk mengurangi jumlah informasi yang tersedia untuk doxxer adalah dengan mempartisi bidang-bidang ini sehingga tidak terhubung satu sama lain. Ini adalah proses yang sangat individual; luangkan waktu untuk mempertimbangkan pertanyaan-pertanyaan berikut dan memetakan lingkup online Anda sendiri.

Apakah Anda menghabiskan waktu Anda untuk menjelajah Facebook dengan topik politik atau halaman debat? Apakah Anda sering menyukai atau memposting ulang status dari akun Instagram atau Twitter radikal? Apakah Anda memiliki gambar atau informasi pribadi di papan pekerjaan? Apakah Anda membeli barang di Etsy atau eBay? Apakah ada teman Anda yang memposting foto Anda di akun Instagram mereka? Apakah Anda harus mempromosikan diri Anda secara online untuk peker-

jaan yang Anda jalani? Apakah Anda terhubung dengan rekan kerja, anggota keluarga, dan teman aktivis Anda menggunakan akun yang sama? Apakah Anda menggunakan bagian dari nama asli atau tanggal lahir Anda untuk nama pengguna atau email?

Masing-masing mungkin tidak menjadi masalah tersendiri, tetapi bersama-sama mereka dapat menciptakan hubungan antara berbagai bidang kehidupan Anda.

Bertanya pada diri sendiri:

- Seberapa terpisahkah masing-masing akun/identitas ini?
- Apa itu publik? Apa itu pribadi?
- Apa yang dimaksud dengan publik dan privat dalam konteks setiap situs?
- Apa yang dapat ditemukan dengan mencari nama resmi Anda?
- Apakah Anda menggunakan nama pengguna atau email yang sama untuk beberapa akun?
- Apakah ini menyeberang ke bidang yang berbeda dari hidup Anda? Luangkan waktu sejenak untuk memikirkan bagaimana semua bidang ini tumpang tindih secara offline.

- Apakah pekerjaan Anda memungkinkan Anda untuk terbuka tentang politik Anda?
- Seberapa publik aktivisme Anda? Apakah Anda berbicara dengan wartawan? Apakah Anda bekerja di sebuah infoshop?
- Apakah Anda memfilter sebagian atau semua konten media sosial Anda dari kerabat?
- Apakah ada referensi tentang aktivitas ilegal atau kontroversial dalam profil tertentu?

Berikut adalah beberapa contoh bagaimana kehadiran online Anda dapat tumpang tindih di berbagai situs:

Kerabat

- Seberapa terbukakah hubungan antara Anda dengan saudara sedarah/sanak saudara yang sah? Jika orang asing memiliki informasi hanya tentang satu orang di jaringan ini, apa yang dapat mereka temukan tentang orang lain?

Politik

- Apakah Anda mendiskusikan atau memposting tentang keyakinan politik Anda secara online? Jika de-

mikian, di platform mana?

Pertemanan dan Komunitas

- Jika Anda memiliki media sosial, siapa teman Anda? Pengikut Anda? Dengan cara apa komunitas online Anda mencerminkan komunitas dunia nyata Anda?

Hobi

- Apa hobi yang Anda miliki? Apakah Anda memiliki teman dan komunitas melalui mereka? Apakah Anda bagian dari komunitas internet yang didedikasikan untuk hobi tersebut?

Legal

- Siapa kamu di atas kertas? Nama, nomor telepon, dan alamat apa yang terikat dengan Anda? Apakah ada akun Anda yang menyertakan informasi ini? Apakah ada situs lain (mungkin tanpa izin Anda)?

Karir

- Apakah pekerjaan Anda melibatkan kehadiran on-

line, situs web, atau akun media sosial? Apakah akan ada masalah jika politik Anda tumpang tindih dengan karir Anda? Atau apakah karier Anda terkait dengan identitas politik Anda?

Luangkan waktu untuk mempertimbangkan di mana Anda tumpang tindih, apa tujuan online Anda, dan di mana Anda dapat memisahkan bidang ini.

Taktik

Mari kita bicara tentang cara menemukan informasi apa yang tersedia tentang Anda, cara mengidentifikasi dan menghilangkan jejak, dan sumber daya online apa yang ada untuk menghapusnya.

Mulailah dengan apa yang tersedia untuk umum. Google sendiri dan buat daftar semua akun media sosial Anda. Hapus akun lama untuk hal-hal yang tidak lagi Anda gunakan. Ini juga saat yang tepat untuk mengunduh pengelola kata sandi seperti ***1Password*** atau ***LastPass*** untuk membantu Anda mengelola nama pengguna, email, dan kata sandi yang unik.

Hapus Situs *Snoop* / Broker Data

Cari tahu informasi apa yang dapat diketahui orang tentang Anda hanya dengan menggunakan mesin pencari. Cari sendiri di DuckDuckGo dan Google. Coba lakukan penelusuran ini dalam mode penyamaran. Coba versi yang berbeda dari nama Anda, dengan dan tanpa nama tengah Anda dan dalam tanda kutip. Anda dapat mengatur Google Alerts untuk mengirimi Anda email saat nama Anda dipublikasikan di internet. Ini akan memberi Anda gambaran tentang seberapa banyak data tentang Anda yang tersedia secara online untuk orang-orang yang tidak berada dalam jaringan Anda.

Setelah pencarian awal ini, lihat semua situs pialang data yang mendapat untung dari perdagangan data pribadi. Saya juga mendorong Anda untuk menghapus anggota keluarga terdekat Anda pada saat yang sama. Proses ini bisa jadi sulit; situs-situs ini berusaha mempersulit penghapusan informasi tentang diri Anda. Ada beberapa hal yang tidak dapat Anda hapus sendiri—misalnya, jika Anda baru saja mendaftar untuk memilih dan masih tinggal di alamat tersebut. (Ini adalah alasan lain mengapa beberapa orang memilih untuk tidak memilih.)

Situs host yang paling banyak diperdagangkan meliputi: Been-verified, CheckPeople, Instant Checkmate, Intelius, PeekYou, PeopleFinders, PeopleSmart, Pipl, PrivateEye, PublicRecords360, Radaris, Spokeo, USA People Search, TruthFinder.com, Nuwber, and FamilyTreeNow. Saya sarankan memulai dengan mencari sendiri di OneRep menggunakan versi gratis dari layanan mereka—ini akan menunjukkan kepada Anda situs apa yang memiliki informasi Anda. Kemudian gunakan informasi itu di situs web ini, yang memiliki panduan untuk memilih keluar dari hampir setiap broker data. Jika Anda memiliki lebih banyak uang daripada waktu, Anda dapat membayar OneRep atau Just Delete Me agar informasi Anda dihapus, tetapi saya biasanya hanya merekomendasikan layanan ini jika Anda telah didoxx.

Saya sarankan memulai dengan ini dengan mencari masing-masing di situs web ini, yang memiliki panduan untuk memilih keluar dari hampir setiap broker data. Jika Anda memiliki lebih banyak uang daripada waktu, Anda dapat membayar layanan yang disebut Just Delete Me agar informasi Anda dihapus, tetapi saya biasanya hanya merekomendasikan layanan ini jika Anda telah didoxx.

Hapus Akun Lama

Saat Anda mencari sendiri di mesin pencari online, Anda mungkin juga menemukan akun lama. Sebaiknya lakukan pencarian terbalik menggunakan semua nama pengguna lama dan nama layar yang dapat Anda ingat. Akun yang sudah lama tidak Anda gunakan dapat membuat Anda rentan karena jika mereka menggunakan kata sandi yang lebih lama, mereka dapat mencoba dukungan teknis akun tersebut untuk mendapatkan lebih banyak data tentang Anda yang dapat mereka coba gunakan untuk akun lain. Unduh materi apa pun yang bernilai sentimental untuk Anda dan tutup secara permanen semua akun yang tidak lagi Anda gunakan. Ini bisa penuh dengan petunjuk tentang hidup Anda.

Pertama, buka situs web ini, yang menelusuri lebih dari ratusan platform untuk nama pengguna tertentu, dan cari semua kemungkinan nama pengguna dan email yang telah Anda gunakan. Ini akan memberi tahu Anda platform apa yang memiliki akun menggunakan pegangan itu.

Kedua, buka di sini dan ketik domain situs web. Situs web ini mengarsipkan sejumlah besar situs web yang ada, mengkategorikan seberapa mudah atau sulitnya mengha-

pus akun, dan menyediakan tautan ke halaman "hapus profil" untuk setiap situs masing-masing.

Haveibeenpwned.com akan membantu Anda mengetahui apakah ada pelanggaran data yang melibatkan akun yang Anda pegang. Jika ada, segera ambil tindakan untuk mengubah kata sandi.

Ubah Nama Pengguna, Alamat Email, dan Kata Sandi

Cara termudah bagi seseorang untuk menemukan lebih banyak informasi tentang Anda adalah dengan mencari nama, alias, dan nama pengguna Anda. Untuk memisahkan lingkup aktivitas internet Anda, selalu gunakan nama pengguna baru saat Anda membuat akun. Jika Anda memiliki situs web profesional untuk bekerja dan harus menggunakan nama resmi Anda, pastikan email yang Anda gunakan untuk akun tersebut hanya digunakan untuk tujuan tersebut. Anda mungkin harus memiliki beberapa akun email dan nama pengguna. Saya memiliki satu untuk semua akun medis dan pemerintahan saya, satu untuk belanja online saya, satu untuk kehidupan politik saya, dan satu untuk media sosial saya, satu lagi untuk situs kencan, dan seterusnya. Saya menggunakan

alias dan informasi palsu untuk semua situs web yang mewakili saya atau menampilkan foto saya.

Pengelola kata sandi sangat membantu untuk ini, karena akan menyimpan login untuk semua akun Anda. Saya merekomendasikan ***LastPass***, yang dapat Anda unduh untuk ponsel dan browser web Anda. Mungkin tergoda untuk membiarkan diri Anda masuk secara permanen, tetapi selalu pastikan untuk keluar setelah Anda selesai menggunakannya. Pertama, agar Anda tidak lupa kata sandi utama—dan juga untuk memastikan bahwa meskipun seseorang berhasil mendapatkan akses ke ponsel atau komputer Anda, mereka tidak dapat mengakses semua data pribadi Anda. Luangkan waktu ini untuk membuat email baru dan mengubah nama pengguna untuk semua akun yang tidak akan Anda hapus. Anda dapat dengan mudah membuat email baru menggunakan ***Protonmail***. Baik ***1Password*** dan ***LastPass*** dapat membantu menghasilkan kata sandi yang acak, yang paling aman.

Kurasi Apa yang Tersedia dan Ubah Pengaturan Privasi Anda

Setelah Anda menghilangkan semua ujung longgar Anda, lihatlah apa yang Anda pilih untuk dipertahankan dan

apa yang dapat ditemukan di sana. Jika Anda menyimpan akun media sosial apa pun, buka profil Anda dan catat apa yang dapat diketahui orang tentang Anda. Anda dapat memilih dari berbagai strategi tentang cara mendekati ini, tergantung pada seberapa berhati-hati Anda ingin menjadi dan seberapa yakin bahwa mungkin untuk menjaga berbagai bidang aktivitas internet Anda berbeda.

Beberapa pilihan Anda meliputi:

- Menghapus semua foto diri Anda, hewan peliharaan Anda, mobil Anda, kotak surat Anda, tato, dan apa pun yang menyertakan informasi pengenal yang tidak perlu—terutama gambar profil publik Anda.
- Menghilangkan atau memalsukan detail pribadi apa pun di profil Anda—berikan tanggal lahir yang tidak akurat atau tidak ada tanggal lahir sama sekali, pilih jawaban acak untuk kota asal Anda, sekolah yang pernah Anda ikuti, dan informasi lainnya.
- Menghapus pengikut dan teman yang meragukan. Jika Anda mengubah semua pengaturan media sosial Anda menjadi pribadi dan Anda merasa yakin dengan daftar pengikut Anda, mungkin ada lebih sedikit alasan untuk menyembunyikan wajah Anda. Saya tetap menyarankan untuk menyimpan detail tentang

lokasi Anda dan kehidupan pribadi yang intim secara offline. Ingat, Anda hanya seaman orang yang paling terbuka dalam hidup Anda. Jika Anda memilih untuk lebih publik, pisahkan teman dan keluarga Anda, jangan memposting foto mereka atau informasi pribadi mereka tanpa persetujuan mereka, dan ingat bahwa hubungan sosial dapat dilihat melalui jejaring sosial dan situs web pengumpulan data.

Ketika Anda merasa sudah selesai, mintalah seorang teman untuk mencoba membuat profil berdasarkan informasi apa yang dapat mereka temukan tentang Anda sambil berpura-pura menjadi "doxxer" untuk melihat apakah ada sesuatu yang tidak terpikirkan oleh Anda. Mungkin penting untuk secara berkala memeriksa apa yang dapat ditemukan dengan mencari nama Anda setiap beberapa bulan.